



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,957	09/03/2004	Alexander Shipp	117-517	1437
23117, 7590, 02/05/2008 NIXON & VANDERHYE, PC 901 NORTH GLEBE ROAD, 11TH FLOOR ARLINGTON, VA 22203			EXAMINER RAYYAN, SUSAN F	
			ART UNIT 2167	PAPER NUMBER
			MAIL DATE 02/05/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/500,957

Applicant(s)

SHIPP, ALEXANDER

Examiner

Susan F. Rayyan

Art Unit

2167

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 November 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,3-7 and 9-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-7 and 9-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a). Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Claims 1, 3-7, 9-13 are pending.

#### ***Claim Rejections - 35 USC § 101***

2. Claims 7, 9-12 are method claims.

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

the claimed invention is directed to non-statutory subject matter.

Claims 1, 3-6, 13 are directed to non-statutory subject matter.

Regarding claims 1, 3-6 the claims are directed to software per se. Each of the means for elements are software per se.

Claim 13, is a system for processing a computer file ... the system comprising an engine. The engine is software per se. An example of an engine is found in US 2003/003402, as monitoring software engines.

#### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-7, 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication Number 2004/0088570 issued to Guy William Welch Roberts et al ("Roberts") in view of US Patent Application Publication Number 2004/0117401 issued to Kenichi Miyata et al ("Miyata").

**As per claim 1, Roberts teaches:**

A system for processing a computer file to determine whether it contains a virus or other malware comprising:

a) means for generating data with regard to the file to characterize its identity and for thereby referencing a computer database to determine whether it is an instance of a known file (see paragraph 37, lines 8-13checksum equates to "characterize its identity and compare the checksum against new checksum);

b) means for selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware (paragraph 37-38, and Figure 6, Reference Number 42-48, generate a checksum of the file user requested and compare the checksum against stored checksum, if result is the same then there is no re-scanning however if the results are different the file is re-scanned for viruses);

c) means for determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors ...

(paragraph 37, lines 8-18, uses dates and other information to determine currency and status);

and for controlling the means b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the means b) at all (paragraph 38, lines 1-10, if a checksum indicates no change file supplied to user however if a change is detected the file is re-scanned for viruses).

Roberts does not explicitly teach factors including the length of time which the database indicates that the file has been known without malware-containing instances of it being detected. Miyata does teach this limitation (paragraph 24, lines 34 as values are used to determine necessity of scanning; paragraph 25, last scan time as an attribute of a file; paragraph 27, as scan server receives a request for a file and determines whether a scan is necessary using the last scan time and last update time) to eliminate unnecessary scans to accelerate file access. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Roberts with Miyata to eliminate unnecessary scans to accelerate file access as described by Miyata (paragraph 0005).

As per claims 3, 9 same as claim arguments above and Roberts teaches:

wherein the means c) performs said determining of whether a file can be regarded as safe in dependence on factors including sources, recorded in the database, from which instances of the file have originated ( paragraph 34, lines 1-6, Internet address)

As per claims 4, 10, same as claim arguments above and Roberts teaches:

performs said determining of whether a file can be regarded as safe in dependence on factors including the number of times, recorded in the database, instances of the file have been processed (paragraph 37, lines 8-18, checksum comparison and a mechanism which uses dates and other information to determine currency and status).

As per claims 5, 11, same as claim arguments above and Roberts teaches:

means for updating the database in dependence upon the result of the processing of the file by the means b) (paragraph 33, virus found actions include updating).

As per claims 6, 12, same as claim arguments above and Roberts teaches:

wherein the updating of the database, is operative in the event of the means b) determining that the file contains, or is likely to contain, malware to delete the record of the file in the database or to update the record of the file in the database so that the file no longer is taken be safe (paragraph 33, virus found actions).

As per claim 7, same as claim 1 above and Miyata teaches storing the determination of whether or not the file contains, or is likely to contain malware (paragraph 28-29, as current time and scan time are updated).

As per claim 13 Roberts teaches:

an engine that generates data with regard to the file to characterize its identity and for thereby referencing a computer database to determine whether it is an instance of a

known file (see paragraph 37, lines 8-13checksum equates to "characterize its identity and compare the checksum against new checksum);

that processes the file by selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware (paragraph 37-38, and Figure 6, Reference Number 42-48, generate a checksum of the file user requested and compare the checksum against stored checksum, if result is the same then there is no re-scanning however if the results are different the file is re-scanned for viruses);

and that determines, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected (paragraph 37, lines 8-18, checksum comparison and a mechanism which uses dates and other information to determine currency and status);

and for controlling the processing to which the file is subjected such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to the processing at all (paragraph 38, lines 1-10, if a checksum indicates no change file supplied to user however if a change is detected the file is re-scanned for viruses).

### ***Response to Arguments***

5. Applicant's arguments filed November 21, 2007 have been fully considered but they are not persuasive.

Applicant argues prior art of record does not teach "the length of time for which the database indicates the file has been known without malware-containing instance of it being detected". Examiner respectfully disagrees and find Miyata does teach this limitation. In paragraph 26, x indicates a last scan time, paragraph 26, y indicates the last update time of the virus database, paragraph 27, if  $x > y$  file is not scanned because virus free, if last scan time of the file  $>$  last update of virus database time then there is no virus. A comparison of the timestamps must be performed. The difference between the two times is generated to determine a result which would be the length of time the file is without malware.

#### **Contact Information**

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Susan F. Rayyan whose telephone number is 571-272-1675. The examiner can normally be reached on M-F, 7:30-4:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.




Application/Control Number:  
10/500,957  
Art Unit: 2167

Page 8

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
Susan Rayyan  
February 1, 2008

  
JOHN COTTINGHAM  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100